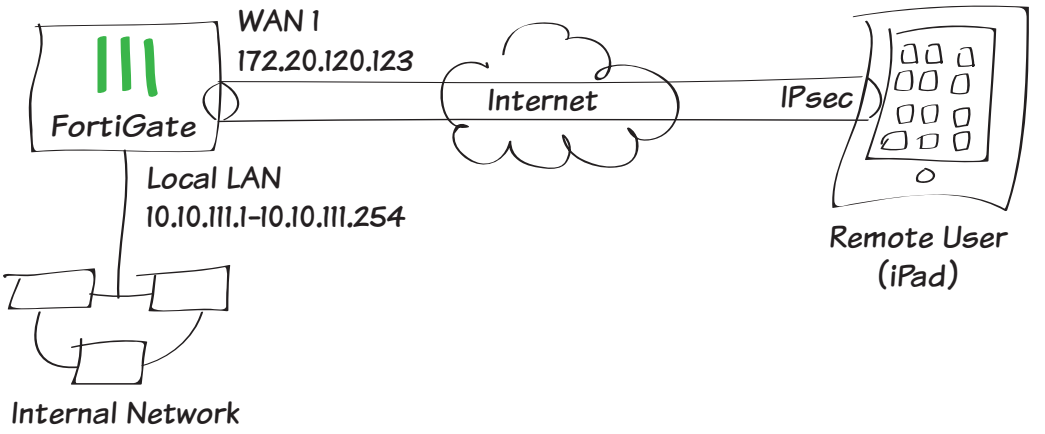
Configuring an IPsec VPN for iOS devices

This recipe uses the IPsec VPN Wizard to provide a group of remote iOS users with secure, encrypted access to the corporate network. The tunnel provides group members with access to the internal network, but forces them through the FortiGate unit when accessing the Internet.

This recipe was tested using an iPad 2 running iOS version 7.1.

1. Creating a user group for iOS users
2. Adding a firewall address for the local network
3. Configuring IPsec VPN using the IPsec VPN Wizard
4. Creating a security policy for access to the Internet
5. Configuring VPN on the iOS device
6. Results

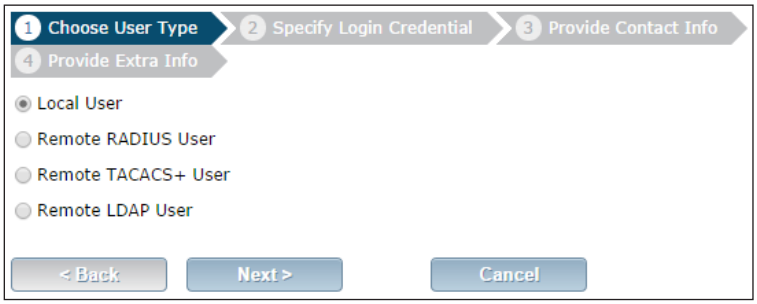


1. Creating a user group for iOS users

Go to **User & Device > User > User Definition**.

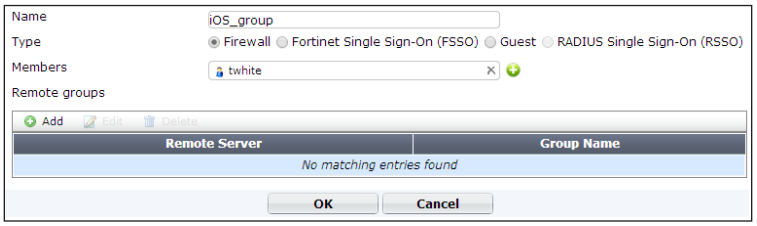
Create a new **Local User** with the User Creation Wizard.

Proceed through each step of the wizard, carefully entering the appropriate information.



Go to **User & Device > User > User Groups**.

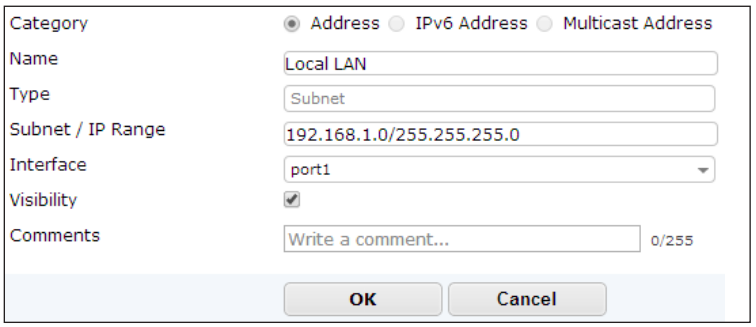
Create a user group for iOS users and add the user you created.



2. Adding a firewall address for the local network

Go to **Policy & Objects > Objects > Addresses**.

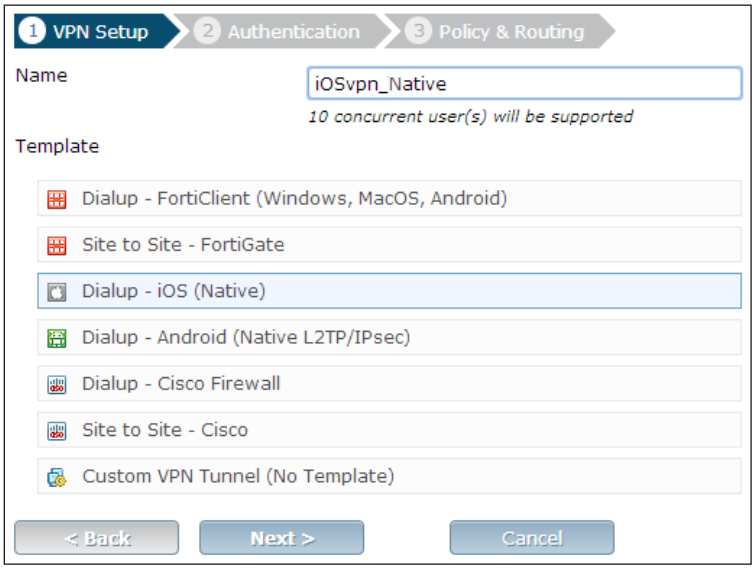
Add a firewall address for the Local LAN, including the subnet and local interface.



3. Configuring the IPsec VPN using the IPsec VPN Wizard

Go to **VPN > IPSec > Wizard**.

Name the VPN connection and select **Dial Up - iOS (Native)** and click **Next**.

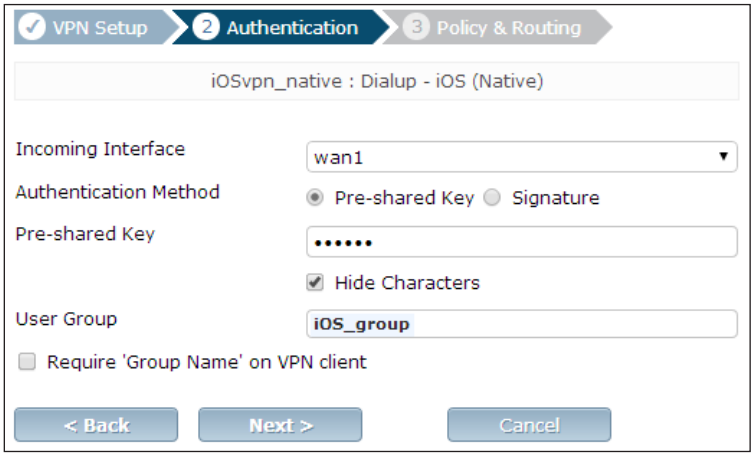


Set the **Incoming Interface** to the internet-facing interface.

Select **Pre-shared Key** for the **Authentication Method**.

Enter a pre-shared key and select the iOS user group, then click **Next**.

The pre-shared key is a credential for the VPN and should differ from the user's password.

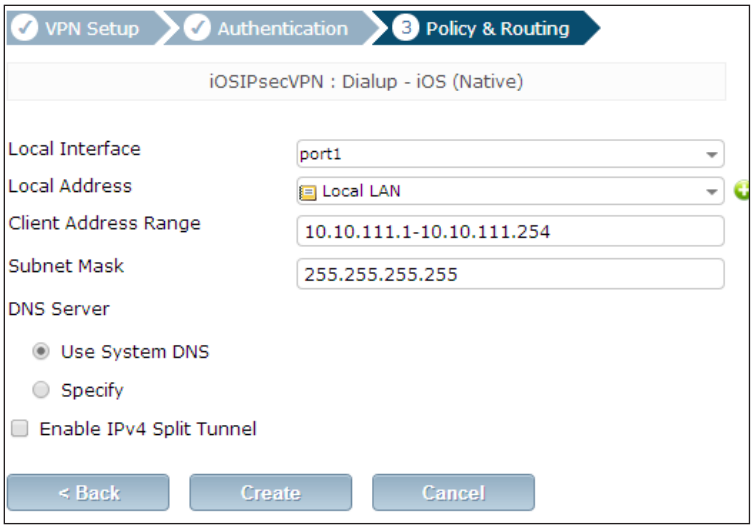


Set **Local Interface** to an internal interface (in the example, port 1) and set **Local Address** to the local LAN address.

Enter an IP range for VPN users in the **Client Address Range** field.

The IP range you enter here prompts FortiOS to create a new firewall object for the VPN tunnel using the name of your tunnel followed by the **_range** suffix (in this case, **iOSvpn_Native_range**).

In addition, FortiOS automatically creates a security policy to allow remote users to access the internal network.



4. Creating a security policy for access to the Internet

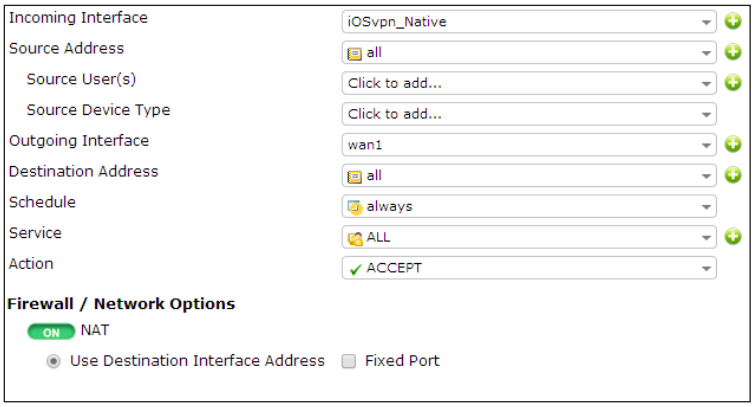
Go to **Policy & Objects > Policy > IPv4**.

Create a security policy allowing remote iOS users to access the Internet securely through the FortiGate unit.

Set **Incoming Interface** to the tunnel interface and set **Source Address** to **all**.

Set **Outgoing Interface** to **wan1** and **Destination Address** to **all**.

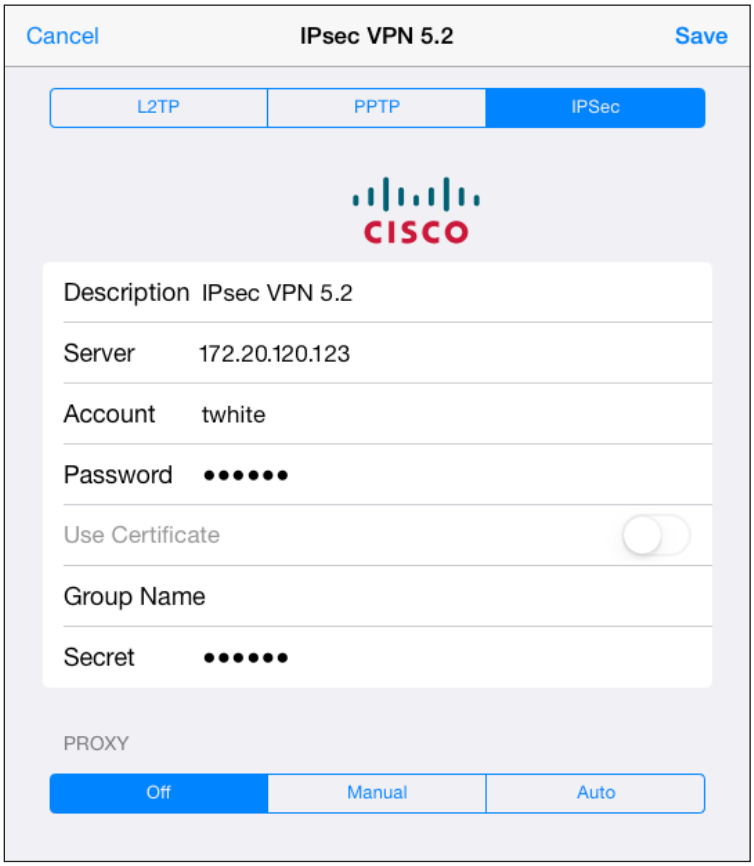
Set **Service** to **all** and ensure that you enable **NAT**.



5. Configuring VPN on the iOS device

On the iPad, go to **Settings > General > VPN** and select **Add VPN Configuration**.

Enter the VPN address, user account, and password in their relevant fields. Enter the pre-shared key in the **Secret** field.



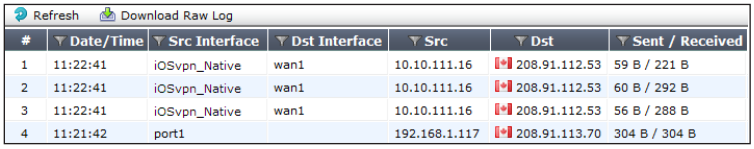
6. Results

On the FortiGate unit, go to **VPN > Monitor > IPsec Monitor** and view the status of the tunnel.

Name	Ty...	Remote Gatew...	Userna...	Stat...	Incoming D.
iOSvpn_Native_0	Dialup	172.20.120.16		Up	9.22 K

Users on the internal network will be accessible using the iOS device.

Go to **Log & Report > Traffic Log > Forward Traffic** to view the traffic.



Refresh Download Raw Log

#	Date/Time	Src Interface	Dst Interface	Src	Dst	Sent / Received
1	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	59 B / 221 B
2	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	60 B / 292 B
3	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	56 B / 288 B
4	11:21:42	port1		192.168.1.117	208.91.113.70	304 B / 304 B

Select an entry to view more information.

Dst	192.168.1.114	**Virtual Domain**	root
Received	72	**Source Country**	Reserved
Sent / Received	72 B / 72 B	**Duration**	63
Sent	72	**Application Details**	
Service	PING	**Protocol**	1
Destination Country	Reserved	**roll**	65428
Status	✓	**Timestamp**	Thu Feb 21 11:20:44 2014
Tran Display	noop	**Sequence Number**	220067
Policy ID	6	**Src Interface**	iOSvpn
Src	10.10.111.16	**VPN**	iOSvpn_Native
Sent Packets	2	**Level**	notice
VPN Type	ipsec-dynamic	**logid**	13
Sub Type	forward	**Threat**	
Received Packets	2	**Date/Time**	11:20:44 (Thu Feb 21 11:20:44 2014)
Dst Interface	port1		

Remote iOS users can also access the Internet securely via the FortiGate unit.

Go to **Log & Report > Traffic Log > Forward Traffic** to view the traffic.

Refresh Download Raw Log

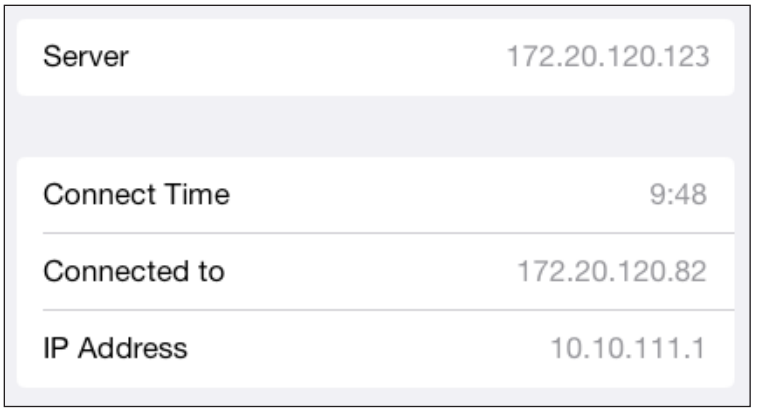
#	Date/Time	Src Interface	Dst Interface	Src	Dst	Sent / Received
1	11:28:43	ios_P1	wan1	10.10.111.16	74.121.50.17	1023 B / 579 B
2	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	59 B / 221 B
3	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	60 B / 292 B
4	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	56 B / 288 B
5	11:20:42	iOSvpn_Native	wan1	10.10.111.16	173.194.73.105	812 B / 642 B
6	11:20:42	iOSvpn_Native	wan1	10.10.111.16	74.125.134.102	808 B / 712 B
7	11:20:42	iOSvpn_Native	wan1	10.10.111.16	173.194.73.94	2.96 KB / 23.07 KB
8	11:20:35	iOSvpn_Native	wan1	10.10.111.16	17.149.36.134	104 B / 60 B
9	11:19:15	iOSvpn_Native	wan1	10.10.111.16	204.93.33.67	813 B / 365 B

Select an entry to view more information.

Dst	74.121.50.17	**Virtual Domain**	root
Received	579	**Source Country**	Reserved
Src NAT IP	172.20.120.123	**Sent / Received**	1023 B / 579 B
Duration	2	**Sent**	1023
Src NAT Port	50189	**Application Details**	
Service	HTTP	**Protocol**	6
Destination Country	United States	**Dst Port**	80
roll	65428	**Status**	close
Timestamp	Thu Feb 21 11:28:43 2014	**Tran Display**	snat
Sequence Number	221594	**Policy ID**	7
Src Interface	iOSvpn_Native	**Src**	10.10.111.16
VPN	iOSvpn	**Sent Packets**	6
Level	notice	**VPN Type**	ipsec-dynamic
Src Port	50189	**logid**	13
Sub Type	forward	**Threat**	
Received Packets	4	**Date/Time**	11:28:43 (Thu Feb 21 11:28:43 2014)
Dst Interface	wan1		

You can also view the status of the tunnel on the iOS device itself.

On the device, go to **Settings > VPN > Status** and view the status of the connection.



Lastly, using a Ping tool, you can send a ping packet from the iOS device directly to an IP address on the LAN behind the FortiGate unit to verify the connection through the VPN tunnel.